Please amend the claims as follows:

1.   (Currently Amended) A computer-implemented method of authenticating the identity of a user, comprising:

          operating a processor operable to perform the following steps:

          a. receiving information identifying a user <u>being authenticated</u>;

          b. obtaining from a biometric contact sensor a data set of biometric contact characteristics for each of a plurality of body parts;

          c. comparing each data set of biometric contact characteristics with authentic versions stored in a database to determine whether each data set of biometric contact characteristics belongs to the user whose <u>identity</u> information was received;

          d. determining whether each of the plurality of body parts of the user was placed on the biometric contact sensor at a sensing position within a predetermined period of time of one another when it is determined that each data set of biometric contact characteristics belongs to the user for which information was received;

          e. determining whether the plurality of parts of the user's body were placed on the biometric contact sensor at the sensing position in a sequence when it is determined that the plurality of parts of the user's body are placed on the biometric sensor within the predetermined period of time of one another, wherein the sequence randomly changes after each authentication of the identity of the user; and

          f. issuing an authentication signal when it is determined that the plurality of parts of the user's body are placed on the biometric contact sensor at the sensing position in the sequence.

2.   (Previously Presented) The method according to claim 1, wherein the body parts are the user's fingertips and the biometric contact sensor is a fingerprint sensor.

3.   (Cancelled)

4.   (Cancelled)

5.   (Previously Presented) The method according to claim 1, wherein the data sets are compared with the authentic versions using a minutiae based algorithm.

6.   (Previously Presented) The method according to claim 1, wherein the data sets are compared with the authentic versions using a correlation based algorithm.

7.   (Currently Amended) An apparatus for authenticating a user, the apparatus comprising a fingerprint sensor operable to sensing only one fingerprint at a time a database, and a processor adapted to perform the steps of:

      a. receiving information identifying a user being authenticated;

      b. obtaining from a biometric contact sensor a data set of biometric contact characteristics for each of a plurality of body parts;

      c. comparing each data set of biometric contact characteristics with authentic versions stored in a database to determine whether each data set of biometric contact characteristics belongs to the user whose identity information was received;

      d. determining whether each of the plurality of body parts of the user was placed on the biometric contact sensor at a sensing position within a predetermined period of time of one another when it is determined that each data set of biometric contact characteristics belongs to the user for which information was received;

      e. determining whether the plurality of parts of the user's body were placed on the biometric contact sensor at the sensing position in a sequence when it is determined that the plurality of parts of the user's body are placed on the biometric sensor within the predetermined period of time of one another, wherein the sequence randomly changes after each authentication of the identity of the user; and

      f. issuing an authentication signal when it is determined that the plurality of parts of the user's body are placed on the biometric contact sensor at the sensing position in the sequence.

8.   (Previously Presented) The apparatus according to claim 7, wherein the fingerprint sensor is a capacitive sensor.

9.   (Previously Presented) The apparatus according to claim 7, wherein the fingerprint sensor is an optical sensor.

10.   (Previously Presented) The apparatus according to claim 7, wherein the fingerprint sensor is a thermal sensor.

11.   (Previously Presented) The apparatus according to any of claim 7, further comprising a data input device.

12.   (Previously Presented) The apparatus according to claim 11, wherein the data input device is a keypad.

13.   (Previously Presented) The apparatus according to claim 11, wherein the data input device is a smart card reader.

14.   (Currently Amended) A method of authenticating the identity of a user, the method comprising:

a. receiving information identifying a user being authenticated

b. obtaining a sequence of data sets of biometric characteristics of the user, each data set relating to one of a plurality of parts of the user's body;

c[[b.]] comparing each data set of biometric contact characteristics with authentic versions stored in a database to determine whether each data set of biometric contact characteristics belongs to the user, wherein the user provided identifying information;

d[[c.]] monitoring the order in which the sequence of data sets was obtained;

e[[d.]] determining whether the data sets are obtained within a predetermined period of time of one another when it is determined that each data set of biometric contact characteristics belongs to the user for which identifying information was provided;

f[[e.]] determining whether the sequence of data sets are in a specified order when it is determined that the data sets are obtained within the predetermined period of time of one another, wherein the specified order changes after each authentication of the identity of the user; and

g[[f.]] issuing an authentication signal when it is determined that the sequence of the data sets are in the specified order.

15.   (Previously Presented) The method according to claim 14, wherein at least one of the plurality of parts of the user's body is a fingertip.

4

16.   (Previously Presented) The method according to claim 14, wherein at least one of the plurality of parts of the user's body is a retina.

17.   (Previously Presented) The method according to any of claim 14, wherein at least one of the plurality of parts of the user's body is the user's face.

18.   (Currently amended) A computer program product for authenticating the identity of a user comprising:

a non-transitory computer readable medium;

computer program instructions, recorded on the non-transitory computer readable medium, executable by a processor, for performing the steps of: comprising:

a. receiving information identifying a user being authenticated;

b. obtaining from a biometric contact sensor a data set of biometric contact characteristics for each of a plurality of body parts;

c. comparing each data set of biometric contact characteristics with authentic versions stored in a database to determine whether each data set of biometric contact characteristics belongs to the user whose identity information was received;

d. determining whether each of the plurality of body parts of the user was placed on the biometric contact sensor at a sensing position within a predetermined period of time of one another when it is determined that each data set of biometric contact characteristics belongs to the user for which information was received;

e. determining whether the plurality of parts of the user's body were placed on the biometric contact sensor at the sensing position in a sequence when it is determined that the plurality of parts of the user's body are placed on the biometric sensor within the predetermined period of time of one another, wherein the sequence randomly changes after each authentication of the identity of the user; and

f. issuing an authentication signal when it is determined that the plurality of parts of the user's body are placed on the biometric contact sensor at the sensing position in the sequence.